PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Masanori SATAKE et al.

Application No.: 10/653,217

Filed: September 3, 2003 Docket No.: 116969

For: JOB PROCESSING DEVICE AND DATA MANAGEMENT METHOD FOR THE DEVICE

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-081445 filed on March 24, 2003

In support of this claim, a certified copy of said original foreign application:

__X__ is filed herewith.

_____ was filed on _____ in Parent Application No. _____ filed _____.

_____ will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/mlo

Date: October 2, 2003

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２４日

出願番号
Application Number: 特願２００３－０８１４４５

[ST. 10/C]: [ＪＰ２００３－０８１４４５]

出願人
Applicant(s): 富士ゼロックス株式会社

２００３年　９月１０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７４２２０

【書類名】　特許願

【整理番号】　FE03-00109

【提出日】　平成15年 3月24日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 12/00

【発明者】

【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社海老名事業所内

【氏名】　佐竹　雅紀

【発明者】

【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社海老名事業所内

【氏名】　益井　隆徳

【発明者】

【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社海老名事業所内

【氏名】　横濱　竜彦

【特許出願人】

【識別番号】　000005496

【氏名又は名称】　富士ゼロックス株式会社

【代理人】

【識別番号】　100075258

【弁理士】

【氏名又は名称】　吉田　研二

【電話番号】　0422-21-2340

【選任した代理人】

【識別番号】　100096976

【弁理士】

【氏名又は名称】　石田　純

【電話番号】　0422-21-2340

【手数料の表示】

【予納台帳番号】　001753

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ジョブ処理装置及び該装置におけるデータ管理方法

【特許請求の範囲】

【請求項１】　第１の記憶装置と、

前記第１の記憶装置よりも記憶したデータを高速に消去可能な第２の記憶装置と、

前記第１の記憶装置と前記第２の記憶装置とに、ジョブの実行に供されるジョブデータを振り分けて格納する格納制御部と、

前記格納制御部により前記第２の記憶装置に振り分けて格納されたジョブデータを、所定の消去条件が満足された場合に消去する消去部と、

を備えるジョブ処理装置。

【請求項２】　請求項１に記載のジョブ処理装置であって、

前記格納制御部により前記第１及び第２の記憶装置に振り分けて格納されたジョブデータを読み出して統合するジョブデータ統合部と、

前記ジョブデータ統合部により統合されたジョブデータに基づき、ジョブを実行するジョブ処理部とを備え、

前記ジョブ処理部によるジョブの実行完了を、前記消去部における所定の消去条件とすることを特徴とするジョブ処理装置。

【請求項３】　請求項１に記載のジョブ処理装置であって、

前記第２の記憶装置として揮発性メモリを用いることを特徴とするジョブ処理装置。

【請求項４】　請求項１に記載のジョブ処理装置であって、

前記第２の記憶装置として、前記ジョブ処理装置が備える主記憶装置の一部の領域を利用することを特徴とするジョブ処理装置。

【請求項５】　請求項１に記載のジョブ処理装置であって、

前記格納制御部は、前記ジョブデータを暗号化し、その暗号化結果のデータを前記第１の記憶装置と第２の記憶装置とに振り分けて格納することを特徴とするジョブ処理装置。

【請求項６】　請求項１に記載のジョブ処理装置であって、

前記格納制御部は、所定のルールに従って前記第１の記憶装置と前記第２の記憶装置とにジョブデータを振り分けて格納し、

前記所定のルールを変更するルール管理部を更に備えるジョブ処理装置。

【請求項７】　請求項６に記載のジョブ処理装置であって、

前記ルール管理部は、自装置の状態に応じて前記所定のルールを変更することを特徴とするジョブ処理装置。

【請求項８】　請求項6に記載のジョブ処理装置であって、

前記ルール管理部は、前記ジョブの属性に応じて前記所定のルールを変更することを特徴とするジョブ処理装置。

【請求項９】　請求項１に記載のジョブ処理装置であって、

前記消去部による前記第２の記憶装置に振り分けて格納されたジョブデータの消去後に、前記第１の記憶装置に振り分けて格納されたジョブデータを消去する残消去部を備えることを特徴とするジョブ処理装置。

【請求項１０】　ジョブの実行に供されるジョブデータを記憶装置に格納する格納制御部と、

前記格納制御部により前記記憶装置に格納されたジョブデータの一部を、所定の消去条件が満足された場合に消去する消去部と、

を備えるジョブ処理装置。

【請求項１１】　請求項１０に記載のジョブ処理装置であって、

前記記憶装置からジョブデータを読み出し、読み出したジョブデータを用いて前記ジョブを実行するジョブ処理部を備え、

前記ジョブ処理部によるジョブの実行完了を、前記消去部における所定の消去条件とすることを特徴とするジョブ処理装置。

【請求項１２】　請求項１又は１０に記載のジョブ処理装置であって、

前記消去部における前記所定の消去条件は、ユーザからジョブデータの消去指示を受けることであることを特徴とするジョブ処理装置。

【請求項１３】　請求項１又は１０に記載のジョブ処理装置であって、

前記消去部における前記所定の消去条件は、ユーザからジョブ処理の中止指示を受けることであることを特徴とするジョブ処理装置。

【請求項１４】　請求項１又は１０に記載のジョブ処理装置であって、

ジョブの実行を制御するジョブ制御部であって、前記消去部によるデータ消去処理が完了した時点で別のジョブの実行を許可するジョブ制御部、

を更に備えるジョブ処理装置。

【請求項１５】　ジョブの実行に供されるジョブデータを、第１の記憶装置と、これよりもデータ消去が高速な第２の記憶装置とに振り分けて格納し、

格納された前記ジョブデータのうち前記第２の記憶装置に記憶したデータ部分を、所定の消去条件が満足された場合に消去する、

ことを特徴とするジョブ処理装置のデータ管理方法。

【請求項１６】　コンピュータに、

ジョブの実行に供されるジョブデータを、第１の記憶装置と、これよりもデータ消去が高速な第２の記憶装置とに振り分けて格納する手順と、

格納された前記ジョブデータのうち前記第２の記憶装置に記憶したデータ部分を、所定の消去条件が満足された場合に消去する手順と、

を実行させるためのデータ管理プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コピー機、プリンタ、ファクシミリ、複合機など、ユーザの要求に応じて所定のジョブを実行するジョブ処理装置に関し、特にジョブ処理装置に記憶されるデータの秘密保持のための技術に関する。

【０００２】

【従来の技術】

近年のデジタル複写機や複合機は、ハードディスク等の大容量記憶装置を搭載するものが多い。このような大容量記憶装置は、原稿を複数部数コピーする場合や両面印刷を行う場合に原稿画像を一時的に保存したり、スキャン要求に応じて原稿読取部で読み取った原稿画像をユーザがネットワークを介してダウンロードするまで保存したりするなどの用途に用いられる。

【０００３】

近年、ネットワーク化やこれに伴う情報犯罪の増加を背景として、企業の情報セキュリティ管理強化の気運が高まっており、ＩＳＭＳ(Information Security Management System)などの認証制度も始まっている。ハードディスク抜き取りなどによる情報漏洩リスクを考えると、企業の総合的な情報セキュリティ管理においては、デジタル複写機や複合機の大容量記憶装置内に残ったデータも見過ごせない問題である。

【０００４】

この問題に対し、特許文献１に示される技術では、複写機に機密文書モードを設け、このモードが設定されている時には、画像データの処理が完了した時点でハードディスク上のその画像データを消去することとしている。

【０００５】

また特許文献２に示される技術では、ハードディスクに保存した画像データを複写機のアイドル時間に消去することとしている。

【０００６】

また特許文献３に示される技術では、割込ジョブの画像データを割込復帰前に消去するか、割り込まれたジョブの終了後に消去するかを、その画像データのデータ量に応じて決めている。またこの技術では、ユーザが複写機を利用しない放置時間が所定時間を超えた時にハードディスク上の画像データを消去したり、ユーザが複写の中止を指示した時にその複写処理に係る画像データをハードディスクから消去したりしている。

【０００７】

なお、ハードディスク上の画像データの消去は、単にファイルシステム上でその画像データファイルを削除するだけでは、ハードディスク上に実体データが残るため不十分である。そこで、従来より、ハードディスク上の実体データまで消去する場合は、その実体データの領域にランダムなデータを複数回上書きすることが行われている。

【０００８】

また、画像データを暗号化してからハードディスクに格納することで、更にセキュリティを高めることも行われている。

【０００９】

【特許文献１】

特開平９－２２３０６１号公報

【特許文献２】

特開平９－２８４５７２号公報

【特許文献３】

特開２００３－３７７１９号公報

【００１０】

【発明が解決しようとする課題】

上記特許文献１～３の技術は、いずれも、ハードディスクからの画像データの消去期間中はハードディスクに対する画像データの読み書きができないため、その間は次の印刷処理や画像読取処理を開始することができない。例えばカラーでページ数の多い原稿など、データ量の多い原稿の処理を行った後は、その原稿の画像データを消去するのに長い時間がかかるため、処理待ちが長くなる。特許文献３の技術では、消去処理を行うタイミングを割込その他の条件に応じて制御することで消去処理の影響を低減しようとしているが、いったん消去を始めると消去が完了するまで次の処理を開始できない点は改善されていない。また、特許文献３の技術では、消去処理を実行するタイミングが来るまでの間、ハードディスク中に実体データが完全な形で残っている場合があるという問題があった。

【００１１】

【課題を解決するための手段】

本発明は、第１の記憶装置と、前記第１の記憶装置よりも記憶したデータを高速に消去可能な第２の記憶装置と、前記第１の記憶装置と前記第２の記憶装置とに、ジョブの実行に供されるジョブデータを振り分けて格納する格納制御部と、前記格納制御部により前記第２の記憶装置に振り分けて格納されたジョブデータを、所定の消去条件が満足された場合に消去する消去部と、を備えるジョブ処理装置を提供する。

【００１２】

本発明の好適な態様では、前記第２の記憶装置として揮発性メモリを用いる。

【００１３】

また別の好適な態様では、前記第２の記憶装置として、前記ジョブ処理装置が備える主記憶装置の一部の領域を利用する。

【００１４】

また別の好適な態様では、前記格納制御部は、前記ジョブデータを暗号化し、その暗号化結果のデータを前記第１の記憶装置と第２の記憶装置とに振り分けて格納する。

【００１５】

また別の好適な態様では、ジョブ処理装置は、所定のルールに従って前記第１の記憶装置と前記第２の記憶装置とにジョブデータを振り分けて格納するとともに、前記ルールを変更するルール管理部を更に備える。

【００１６】

ルールの変更は、例えば当該ジョブ処理装置の状態に応じて行うことができる。ここで、ジョブ処理装置の「状態」には、例えば第２の記憶装置の空き容量や書き込み・読み出し速度、ジョブ処理装置の処理負荷、待機中のジョブの有無などがある。

【００１７】

また別の好適な態様では、ジョブ処理装置は、前記ルールを、前記ジョブの属性に応じて変更するルール管理部を更に備える。ここで、ジョブの「属性」には、ジョブに付与された機密度や、ジョブの対象となる文書の種別などがある。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。以下では、本発明の方式を、デジタル複合機などの画像形成装置に適用した場合の例を説明する。すなわち以下では、コピー処理やスキャン処理のための原稿読み取りにより生成された画像データのファイルや、リモートホストから要求された印刷指示やそれを展開した画像データのファイル、受信したファクシミリデータなど、画像形成装置が要求される各種のジョブを実行するために受信したり生成したりしたデータのセキュリティ保護のための仕組みを説明する。

【００１９】

まず、図１を参照して、本実施形態の画像形成装置のハードウエア構成を説明する。図１は、本実施形態の制御の説明のために必要な構成要素を図示したものであり、その他の構成要素については図示を省略している。

【００２０】

この画像形成装置は、ディジタル複写機やディジタル複合機など、原稿を光学的に読み取って得た画像をディジタルデータとして取り扱うタイプの装置である。

【００２１】

この装置においてＲＯＭ（リード・オンリ・メモリ）１２には、この画像形成装置の動作制御のための制御プログラムなどのデジタル情報が格納されている。ＣＰＵ（中央処理装置）１０がこのＲＯＭ１２内の制御プログラムを実行することにより、画像形成装置の各部の制御が実現される。後述するファイルの格納、読み出し、及び消去の各手順を記述したプログラムも、このＲＯＭ１２に格納されている。

【００２２】

ＲＡＭ（ランダム・アクセス・メモリ）１４は、この画像形成装置の主記憶装置であり、制御プログラムの実行の際にワークメモリとしても用いられる。ＲＡＭ１４は、例えば、プリントエンジン２４に供給する１ページ分の画像データを蓄えるページバッファとして用いることもできる。

【００２３】

ＨＤＤ（ハードディスク・ドライブ）１６は、各種のデータを保存するための補助記憶装置である。例えば、ＨＤＤ１６には、画像形成装置が、要求される各種ジョブのために受信したり生成したりしたジョブデータが保存される。このようなジョブデータとしては、例えば、コピーのためにスキャンエンジン２２で読み取った原稿画像データや、リモートホストから依頼された親展プリント処理（ユーザ認証が成功して初めて印刷を行う処理）の印刷指示データやこれを展開して得られる画像データ、スキャン指示に従ってスキャンエンジン２２で読み取った画像データなどがある。このようなジョブデータのファイルは、ジョブの終了

と共にファイルシステムから削除される。ただし、ファイルシステム上で単にファイルを削除しただけではそのファイルの実体データがＨＤＤ上に残るというのが従来からの問題であり、本実施形態ではその問題に対する新たな解決を提供する。

【００２４】

操作パネル１８は、この画像形成装置のユーザインタフェースのための表示や、ユーザからの各種指示の入力受付などのためのユーザインタフェース手段である。操作パネル１８は、典型的には、コピースタートボタンなどの機械的な操作ボタンや液晶タッチパネルを備える。液晶タッチパネルは、ＣＰＵ１０で実行される制御プログラムが生成したＧＵＩ（グラフィカルユーザインタフェース）画面を表示し、そのディスプレイに対するユーザのタッチ位置を検出して制御プログラムに渡す。制御プログラムは、そのタッチ位置の情報からユーザの入力内容を解釈する。

【００２５】

通信インタフェース２０は、ローカルエリアネットワークなどのネットワークとのデータ通信のための制御を行う装置である。リモートホストからのプリント指示等は、この通信インタフェース２０を介して画像形成装置内に入力される。

【００２６】

スキャンエンジン２２は、原稿を光学的に読み取って電子的な画像データを生成するスキャナ機能を提供する装置である。自動原稿送り装置（ＡＤＦ）（図示省略）にセットされた原稿は、ＡＤＦの機能により１枚ずつスキャンエンジンに送られ、光学的に読み取られる。

【００２７】

プリントエンジン２４は、ＣＰＵ１０の制御により供給される画像データを用紙に画像形成（印刷）するプリンタ機能を提供する装置である。

【００２８】

このような画像形成装置において、本実施形態では、保存するジョブデータファイルのセキュリティ向上のための方策として、従来ＨＤＤ１６に格納されていたジョブデータのファイルを、ＨＤＤ１６とＲＡＭ１４とに振り分けて格納する

構成をとる。すなわち、１つのジョブデータファイルは、ＨＤＤ１６内の格納ファイル４０と、ＲＡＭ１４内の格納ファイルの一部分４２とに分けて記憶されることになる。この構成によれば、ジョブデータファイルを消去する場合には、ＲＡＭ１４上の格納ファイルの一部分４２を消去すればよい。ＲＡＭ１４内のデータの消去は高速に行うことができる。ＲＡＭ１４内のデータ４２を消去した場合、ＨＤＤ１６内に残った格納ファイル４０だけでは、元のジョブデータファイルを復元できないので、ジョブデータの秘密を守ることができる。特に、ジョブデータファイルを暗号化してからＨＤＤ１６とＲＡＭ１４とに分散格納する構成とすれば、ＨＤＤ１６に残った格納ファイル４０は、暗号化したジョブデータファイルから一部を欠落させたものなので、復号処理が非常に困難となり、高いセキュリティを実現できる。

【００２９】

図２は、この画像形成装置におけるジョブデータファイルの記憶・読み出し・消去のための機構を示す機能ブロック図である。

【００３０】

この構成において、ジョブ制御部１００は、操作パネル１８や通信インタフェース２０から入力されるジョブ要求を受け付け、それら要求に対応するジョブ処理の実行を制御する。ジョブの実行としては、画像形成処理や種々の画像処理、文字認識処理、他装置への送信処理等が挙げられる。実行中のジョブに対する割込ジョブの受付や、その割込に伴うジョブの退避や復帰の制御も、このジョブ制御部１００により行われる。また、ジョブ制御部１００は、実行するジョブが、ジョブデータの一時保存が必要な場合、その保存を格納・消去処理部１１０に要求する。なお、ジョブデータの一時保存が必要なジョブには、例えば原稿を複数部数コピーするジョブや、親展プリントのジョブ、あるいは読み取った画像を親展ボックスに一時保管するジョブなどがある。複数部数コピーの場合は、その部数分の印刷出力が完了した時点でジョブが完了し、親展プリントの場合は、画像形成装置でのユーザ認証が成功して印刷出力が完了した時点でジョブが完了する。また、親展ボックスへのスキャン画像の保存処理は、リモートホストがその親展ボックス内のデータをダウンロードした時点でジョブが完了する。

【００３１】

また、ジョブ制御部１００は、いったん保存したジョブデータをジョブ実行のために使用する時が来た場合には、格納・消去制御部１１０に対してそのジョブデータの読み出しを要求する。

【００３２】

格納・消去制御部１１０は、ジョブデータファイルの格納及び読み出しの処理を行うモジュールである。ジョブ制御部１００からジョブデータファイルの格納要求があった場合は、格納・消去制御部１１０は、それらを所定の振り分けルール（又は手順）に従ってＲＡＭ１４とＨＤＤ１６に分散格納する。またジョブ制御部１００からジョブデータファイルの読み出し要求があった場合は、格納・消去制御部１１０は、ＲＡＭ１４とＨＤＤ１６に分散格納したデータを読み出し、振り分けルールに基づいて統合することで元のジョブデータファイルを復元し、ジョブ制御部１００に提供する。

【００３３】

暗号処理部１１２は、格納・消去制御部１１０によりＲＡＭ１４やＨＤＤ１６に格納するデータを所定の暗号アルゴリズムに従って暗号化したり、ＲＡＭ１４やＨＤＤ１６から読み出したデータを復号したりする。

【００３４】

乱数発生部１１４は、格納・消去制御部１１０によるＲＡＭ１４及びＨＤＤ１６への分散格納処理のために乱数を発生させるモジュールである。

【００３５】

メモリ監視部１１６は、ＲＡＭ１４の空き容量を監視するモジュールである。監視により求めた空き容量の情報は、格納・消去制御部１１０が、ジョブデータのＲＡＭ１４とＨＤＤ１６への振り分け量を求めるのに利用される。

【００３６】

次に図３を参照して、格納・消去制御部１１０によるジョブデータファイルの格納時の処理を説明する。

【００３７】

ジョブ制御部１００からジョブデータファイルの格納要求を受けた場合、格納

・消去制御部１１０は、まずそのファイルを暗号処理部１１２に暗号化させる（Ｓ１０）。

〔００３８〕

次に格納・消去制御部１１０は、暗号化したジョブデータのうち、ＲＡＭ１４に格納するデータのサイズを計算する（Ｓ１２）。この計算は、メモリ監視部１１６で求めたＲＡＭ１４の空き容量と、乱数発生部１１４で発生させた乱数とを用いて、格納サイズを計算する。基本的な考え方は、ＲＡＭ１４の空き容量が多いほど格納サイズを大きくすると共に、空き容量と格納サイズの関係が一定とならないように乱数を用いて調整を加えるというものである。例えば、ＲＡＭ１４の空き容量の所定割合を格納サイズの基準値と決定し、乱数発生部１１４で発生させた正規分布の乱数によってその基準値に調整を加えることで格納サイズを求める、などの処理となる。格納サイズの決定に際しＲＡＭ１４の空き容量を考慮することで、格納処理の際のワークメモリ不足を回避することができる。また、乱数により格納サイズを変化させることで、分散格納の規則を分かりにくくすることができ、セキュリティの向上が見込める。

〔００３９〕

ＲＡＭ１４への格納サイズの計算が終わると、格納・消去制御部１１０は、暗号化されたジョブデータ（以下、混乱のおそれがない場合には単に「ジョブデータ」と呼ぶ）の先頭からその格納サイズ分のデータをＲＡＭ１４に格納する（Ｓ１４）。このときのＲＡＭ１４におけるデータの格納位置（先頭アドレス）は、ランダムに決定しても良いし、所定のルール（空き容量の先頭に格納するなど）に従って決定しても良い。

〔００４０〕

ＲＡＭ１４への格納の後、格納・消去制御部１１０は、ＨＤＤ１６への格納サイズを計算する（Ｓ１６）。この格納サイズの計算は、ＲＡＭ１４への格納サイズの計算と同様に行えばよい。

〔００４１〕

ＨＤＤへの格納サイズが計算できると、格納・消去制御部１１０は分散管理情報を作成してＨＤＤ１６に書き込むと共に（Ｓ１８）、ジョブデータの未格納部

分の先頭からその格納サイズ分のデータをＨＤＤ１６に書き込む（Ｓ２０）。なお、ＨＤＤ１６中には、画像形成装置のオペレーティングシステムにより、当該ジョブデータを格納するためのファイル領域が確保されており、この領域にそれら分散管理情報とジョブデータとを書き込んでいくことになる。

【００４２】

以上のステップＳ１２～Ｓ２０の処理を、ジョブデータの未格納部分が無くなるまで繰り返す（Ｓ２２）。これにより、ジョブデータがＲＡＭ１４とＨＤＤ１６とに分散格納されることになる。このように、図３の処理では、ジョブデータを少量ずつＲＡＭ１４とＨＤＤ１６とに交互に格納していく。

【００４３】

図３の処理により、ＨＤＤ１６内に生成される格納ファイル４０のデータ構造の例を図４に示す。この図に示すように、格納ファイル４０は、分散管理情報４１０と格納ファイルの部分データ４５０の繰り返しにより構成される。分散管理情報４１０は、ＲＡＭ１４に格納したデータへのアクセスのための情報であり、部分データ４５０は、ジョブデータの一部分である。この部分データ４５０は、例えばＡＳＮ．１のＢＥＲエンコーディング規則に従ったデータ構造で記述される。この場合、部分データ４５０は、当該データの型を示すオブジェクト型４５２の情報と、そのデータのサイズ４５４と、そのデータの値４５６がこの順に並んだものとなる。図３のステップＳ１２からＳ２０の処理を１回行うごとに、分散管理情報４１０とその次の部分データ４５０ができる。

【００４４】

分散管理情報４１０のデータ構造の一例を図５に示す。この例では、分散管理情報４１０は、まずこの管理情報自体の識別子４１２から始まり、その次にその管理情報自体のサイズ４１４が記述され、更にその次に、ジョブデータの分散先のデバイス（本実施形態ではＲＡＭ１４）に格納したデータへのアクセスのための情報４２０が記述される。情報４２０は、分散先デバイスの識別子４２２と、その分散先デバイスに振り分けて記憶したデータのそのデバイス内での記憶位置４２４と、そのデータのデータサイズ４２６とを含んでいる。分散先のデバイスがＲＡＭ１４の場合、記憶位置４２４としては、例えばＲＡＭ１４における当該

データの記憶領域の先頭アドレスを用いることができる。

【００４５】

図１の例では、ジョブデータをＨＤＤ１６とＲＡＭ１４とに分散させた。しかし、画像形成装置がＨＤＤ１６とＲＡＭ１４以外にも記憶装置を備えている場合がある。例えば、画像形成装置がＨＤＤを複数備えていたり、ＥＥＰＲＯＭや不揮発性ＲＡＭを備えていたりする場合もある。このような場合、ジョブデータをそれら複数の記憶装置に分散格納することもできる。分散先デバイスの識別子４２２は、それら複数の記憶装置を識別するためのものである。そして、ジョブデータをＨＤＤ１６以外に複数の記憶装置に分散格納した場合は、分散管理情報４１０には、それら各記憶装置ごとに情報４２０が記述されることになる。この場合、分散管理情報４１０における情報４２０の順序が、分散格納したジョブデータの順序に対応する。

【００４６】

次に図６を参照して、分散格納したジョブデータを読み出す際の格納・消去制御部１１０の処理を説明する。

【００４７】

格納・消去制御部１１０は、ジョブ制御部１００からジョブデータファイルの読み出しを要求された場合、まずＨＤＤ１６内の当該ファイルの先頭にアクセスし（Ｓ３０）、分散管理情報４１０を読み出し、その分散管理情報４１０に示される記憶装置識別子４２２，記憶位置４２４及びデータサイズ４２６の情報に従ってＲＡＭ１４に分散格納したデータを読み出す（Ｓ３２）。なお、分散格納先の記憶装置が複数存在する場合には、分散管理情報４１０中の情報４２０の順に、それら各記憶装置からデータを読み出して併合していく。このようにしてすべての分散格納先の記憶装置からのデータ読み出しが終わると、その分散管理情報４１０の直後に格納された部分データ４５０を読み出し、これを分散先から読み出したデータの後ろに併合する（Ｓ３４）。このような処理を、格納ファイル４０の末尾に達するまで繰り返す（Ｓ３６）ことにより、ジョブデータの読み出しが完了する。なお、読み出したジョブデータは暗号化されているので、格納・消去制御部１１０はこれを暗号処理部１１２に復号させてから、ジョブ制御部１０

０に提供する。

【００４８】

次に図７を参照して、ＨＤＤ１６とＲＡＭ１４に分散格納したジョブデータファイルの消去処理を説明する。

【００４９】

この消去処理は、ジョブデータファイルに関して所定の消去条件が満たされた時に実行される。代表的な消去条件としては、当該ジョブデータファイルを用いるジョブの実行が完了したことを挙げることができる。またジョブデータファイルを用いるジョブの中止指示がユーザより入力されることも消去条件の一例である。また、ユーザがジョブデータファイルを指定し、そのファイルの消去を明示的に指示することも、消去条件の一例である。

【００５０】

格納・消去制御部１１０は、ジョブ制御部１００からのジョブ実行完了通知や、操作パネル１２からのユーザの入力を監視し、それら消去条件のいずれかかが満足されるのを待つ（Ｓ４０，Ｓ４２，Ｓ４４）。そして、いずれかの消去条件が満足された場合、その条件を満足したジョブのジョブデータファイルのうちのＲＡＭ１４に格納された部分４２を消去する（Ｓ４６）。消去部分の特定は、例えば格納ファイル中の分散管理情報４１０を読み出すことで行うことができる。ＲＡＭ１４上のデータなので、高速かつ完全に消去することができる。次に、ＨＤＤ１６内の当該ジョブデータの格納ファイル４０を削除して、その格納ファイルの領域を解放する（Ｓ４８）。この削除処理は、ＭＳ－ＤＯＳ（商標）のＤＥＬコマンドや、ＵＮＩＸ（登録商標）のｒｍコマンドによるファイル削除のように、ファイルシステム上でそのファイルの管理情報を削除する処理でよい。この場合、ＨＤＤ１６には、削除後にも（上書きされるまでは）格納ファイル４０の実体データが残ることになるが、残った実体データだけでは元のジョブデータファイルを完全には復元できない。また、本実施形態では、ジョブデータファイルを暗号化してからＨＤＤとＲＡＭに分散格納しているので、ＨＤＤに残った実体データだけでは復号が非常に困難になる。

【００５１】

格納ファイルの削除（Ｓ４８）が完了すると、格納・消去制御部１１０は、ジョブ制御部１００に対し、要求されたデータ消去処理が完了した旨を通知する（Ｓ５０）。この通知を受けたジョブ制御部１００は、次のジョブの実行を許可する。これにより、例えば消去の時点で待機中のジョブ（新たなジョブや、別のジョブに割り込まれたジョブなど）があれば、そのジョブの実行が開始又は再開される。

【００５２】

このように、本実施形態によれば、ＲＡＭ１４に分散格納したデータを消去することで、ＨＤＤ１６に保存したジョブデータを無効に近い状態とすることができるので、ＨＤＤに保存したジョブデータ全体にランダムデータを何度も上書きしていた従来技術と比べて、はるかに高速にデータ消去を行うことが可能となる。このため、割込ジョブからの復帰時や後続のジョブが待機しているような場合でも、待機中のジョブをほとんど待たせることなく、データ消去を行うことができる。したがって、ジョブデータの消去を次のジョブの完了まで先送りにする必要が無くなる。

【００５３】

また、本実施形態では、ジョブデータの分散格納先として、揮発性メモリであるＲＡＭ１４を用いているので、画像形成装置の電源をオフすれば、分散格納したデータも消えてしまうので、上述の消去処理と同様の効果が得られる。

【００５４】

なお、１つの例として、上述したＲＡＭ１４内のデータ消去のあと、適切なタイミングでＨＤＤ１６上に残った格納ファイルの実体データに対し、ランダムデータの繰り返し上書きによるデータ消去を行うことも好適である。このランダムデータ上書きによる消去処理は、例えば画像形成装置の未使用状態が所定時間続いた時や、節電モードに移行する直前、電源スイッチがオフされた時など、ジョブに影響の少ないときに行うことが好適である。本実施形態では、ジョブ終了後からランダムデータ上書きによるデータ消去を行うまでの間、上記各特許文献に示した従来技術よりもジョブデータを安全に保つことができる。

【００５５】

以上に説明した実施形態では、ＲＡＭ１４に分散格納するデータのサイズをＲＡＭの空き容量と乱数に従って決めていたが、これはあくまで一例である。この代わりに、ＲＡＭ１４への格納サイズを固定値としても良いし、空き容量を考慮せずに完全にランダムに決定しても良い。

【００５６】

また、ＲＡＭ空き容量の他の状況も考慮して格納サイズを決めることも好適である。この例を図８に示す。この例では、ＲＡＭ空き容量（Ｓ６０）の他に、待機中のジョブの有無（Ｓ６２）や、画像形成装置全体の処理負荷（Ｓ６４）、ジョブデータの機密度（Ｓ６６）、などの情報を取得し、これらの情報をパラメータとしてＲＡＭ１４への格納サイズを決める（Ｓ６８）。この計算の基本的な考え方は以下の通りである。

【００５７】

まず、待機中のジョブがある場合や、画像処理装置の処理負荷が高い場合は、ＨＤＤ１６へのランダムデータ上書きによるデータ消去がそれだけ遅くなるため、その消去までの時間のジョブデータの安全性を高めるために、ＲＡＭ１４への振り分け量を多くする。これにより、ジョブ完了後のＲＡＭ内データ消去によって、より多くのデータが消滅することになるので、ジョブデータの復元の可能性をより減らすことができる。

【００５８】

なお、待機中のジョブの有無の情報はジョブ制御部１００から、画像処理装置全体の処理負荷はジョブ制御装置１００やオペレーティングシステムから、それぞれ取得することができる。

【００５９】

また、ジョブデータの機密度が高い場合は、そのデータが不要になった時点で、そのデータのうちできるだけ多くの部分を消すことがセキュリティ上有効である。したがって、機密度が高いほどＲＡＭ１４へのデータの振り分け量を多くする。

【００６０】

ジョブデータの機密度は、ジョブの属性の一つとしてユーザに指定させても良

いし、ジョブの内容から判定しても良い。後者の例としては、例えば親展プリントなど秘密を前提としたジョブの場合は、ジョブデータの機密度を高くするなどである。予めジョブの種類ごとの機密度を画像形成装置に登録しておけばよい。

【００６１】

また、ＨＤＤ１６の他にジョブデータを振り分ける記憶装置が複数ある場合、それら複数の記憶装置への振り分け量をそれら記憶装置への書き込み・読み出し速度に応じて決めることも好適である。各記憶装置への書き込み・読み出し速度は、ジョブデータ全体の格納・読み出しの速度に影響するので、書き込み・読み出しが遅い記憶装置へのデータの振り分け量は相対的に小さくすることが好適である。例えば、ＲＡＭ１４の他に、ＥＥＰＲＯＭにデータを振り分ける場合、ＥＥＰＲＯＭの書き込み・読み出し速度は、ＲＡＭ１４は当然のこと、ＨＤＤ１６と比べても遅いので、ＥＥＰＲＯＭへの振り分け量をＲＡＭへの振り分け量よりも小さいものとする。

【００６２】

また、ジョブデータの内容に応じた振り分け制御も考えられる。例えば、ジョブデータがヘッダ部とデータ部（ボディ部）から構成される形式であり、ヘッダ部にデータの特徴が多く含まれている場合には、ヘッダ部のデータはＲＡＭ１４に多く振り分け、ボディ部のデータはＨＤＤ１６に多く振り分ける、等といった制御などが考えられる。

【００６３】

また、以上では、ジョブデータを暗号処理部１１２で暗号化してから分散格納したが、このような暗号化を行わない場合でも、本発明の分散格納方式はある程度の有効性を持つ。暗号化しなくても、ＲＡＭ１４内のデータ消去により、ジョブデータの一部は消滅するので、万が一ＨＤＤ１６が取り外されるようなことがあっても、完全なジョブデータが漏れることはない。

【００６４】

なお、画像形成装置でジョブデータの暗号化を行わない場合、ジョブデータ自体が暗号化されている場合（例えばホストからの印刷データ自体が暗号化されている場合）と、そうでない場合とで、ＲＡＭ１４とＨＤＤ１６の間のデータ振り

分け割合を変えることも好適である。すなわち、ジョブデータが暗号化されている場合は、ＲＡＭ内のデータ消去でジョブデータのうちのできるだけ多くの情報が消えるよう、ＲＡＭへのデータ振り分け割合を高くするなどである。

【００６５】

また、ジョブデータを暗号化せずに分散格納する場合のＲＡＭ、ＨＤＤ間でのデータの振り分け方法として、ジョブデータがタグ付けされた構造化文書の場合、タグ情報（開始タグ、終了タグのうちの一方でも良いし両方でも良い）をＲＡＭに優先的に振り分ける方法が考えられる。この方法では、ＲＡＭ内のデータ消去により文書構造の情報を消滅させることができる。また、ジョブデータがビジネス文書の場合は文書内の数字情報をＲＡＭに優先的に振り分け、名簿データの場合は人名漢字に該当する文字をＲＡＭに優先的に振り分ける、などと、ジョブデータの種類に応じた特徴部分をＲＡＭに振り分ける方式も好適である。文書の種類は、ジョブデータファイルの属性情報などから求めることができる。

【００６６】

また、以上の例では、ＲＡＭ１４とＨＤＤ１６に交互にジョブデータを振り分けたが、この代わりにそれら両者間での振り分け順序をランダムに変えることも可能である。この場合、分散管理情報４１０には、各分散格納先に記憶したデータの順序の情報を含める。

【００６７】

また以上の例では、分散管理情報４１０をＨＤＤ１６に格納したが、これは必須ではない。分散管理情報４１０のような、各記憶装置へのジョブデータの分散状況を記述した管理情報は、ＲＡＭ１４やその他画像形成装置内の記憶装置に記憶するようにしてもよい。

【００６８】

また本実施形態の変形例として、ＲＡＭ１４を利用しない装置構成も考えられる。この例を図９に示す。図９において、図２に示した構成要素と同一又は類似の構成要素には、同一符号を付して説明を省略する。

【００６９】

この例では、格納・消去制御部１１０ａは、ジョブデータを暗号処理部１１２

で暗号化した後、従来と同様ＨＤＤ１６のみに格納する。

【００７０】

この変形の特徴は、ジョブデータの消去処理にある。すなわち、図１０に示すように、ジョブデータの消去条件が満足された場合（Ｓ４０～Ｓ４４）、格納・消去制御部１１０ａは、乱数発生部１１４に発生させた乱数を用い、ＨＤＤ１６内のジョブデータのうちの消去箇所を決定する（Ｓ５２）。ここでは、発生させた１乃至複数の乱数を用い、複数の消去箇所について、その位置や消去するデータサイズを決定する。そして、格納・消去制御部１１０ａは、それら決定した消去箇所に対して、ランダムなデータを所定数回繰り返し上書きする（Ｓ５４）。この上書き消去が完了すると、格納・消去制御部１１０ａは、当該ジョブデータのファイルをファイルシステム上から削除し、ジョブ制御部１００に対してデータ消去完了の旨を通知する（Ｓ５０）。これにより次のジョブが実行可能な状態となり、待機中のジョブや割込などによる中断中のジョブがあれば、それを実行することができる。また、この消去の後、ＨＤＤ１６内に残ったジョブデータの部分に対し、画像形成装置のアイドル時間などに、ランダムデータの繰り返し上書きによる消去処理を施せば、更にセキュリティを向上させることができる。

【００７１】

本実施形態によれば、ＨＤＤ１６に格納したジョブデータのうちの複数の消去箇所を消去した時点で、ＨＤＤ１６内に残ったジョブデータは完全なものではなくなり、仮にその残りデータが取り出されても秘密漏洩のリスクは少なくなる。

【００７２】

この例では、暗号化したジョブデータの複数の部分を消去するので、残ったデータを復号するのは非常に困難となる。

【００７３】

また、それら消去箇所のサイズのジョブデータ全体に対する比率を小さくしておけば、この消去処理に要する時間は短くて済むため、待機中のジョブをさほど待たせることなく消去処理を実行できる。

【００７４】

以上、本発明をデジタル複合機等の画像形成装置に適用した場合の実施形態を

説明した。しかしながら、上述の説明から明らかなように、本実施形態における格納データの秘密保護方式は、処理の種類や格納対象のデータの種類に依存しないので、画像形成装置以外の様々なジョブ処理装置に適用可能である。

【図面の簡単な説明】

【図１】　実施形態の画像形成装置のハードウエア構成の要部を示す図である。

【図２】　実施形態の画像形成装置におけるジョブデータファイルの記憶・読み出し・消去のための機構を示す機能ブロック図である。

【図３】　格納・消去制御部によるジョブデータファイルの格納処理手順の一例を示すフローチャートである。

【図４】　ＨＤＤ内の格納ファイルのデータ構造の例を示す図である。

【図５】　格納ファイル内の分散管理情報のデータ構造の例を示す図である。

【図６】　分散格納したジョブデータファイルの読み出し手順の一例を示すフローチャートである。

【図７】　ジョブデータファイルの消去処理手順の一例を示すフローチャートである。

【図８】　ＲＡＭへの格納データ量の決定手順の例を示すフローチャートである。

【図９】　ジョブデータの格納・消去のための装置の変形例を示す図である。

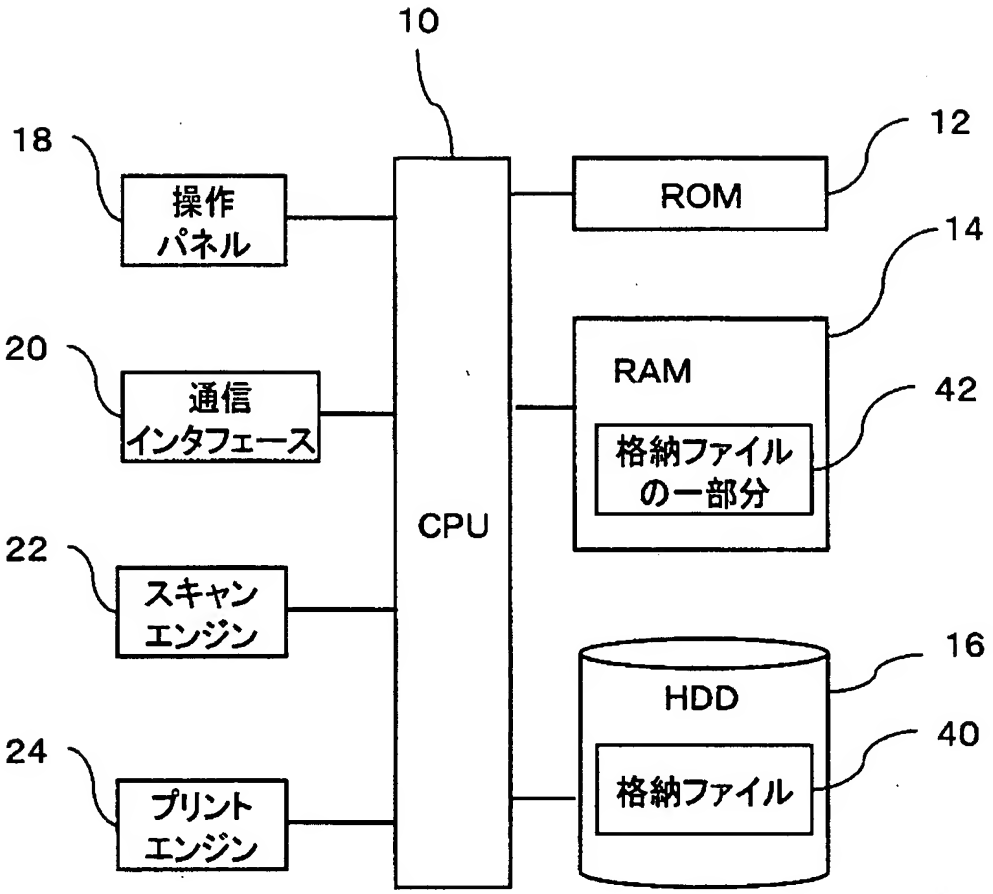
【図１０】　変形例におけるジョブデータファイルの消去処理手順の一例を示すフローチャートである。

【符号の説明】

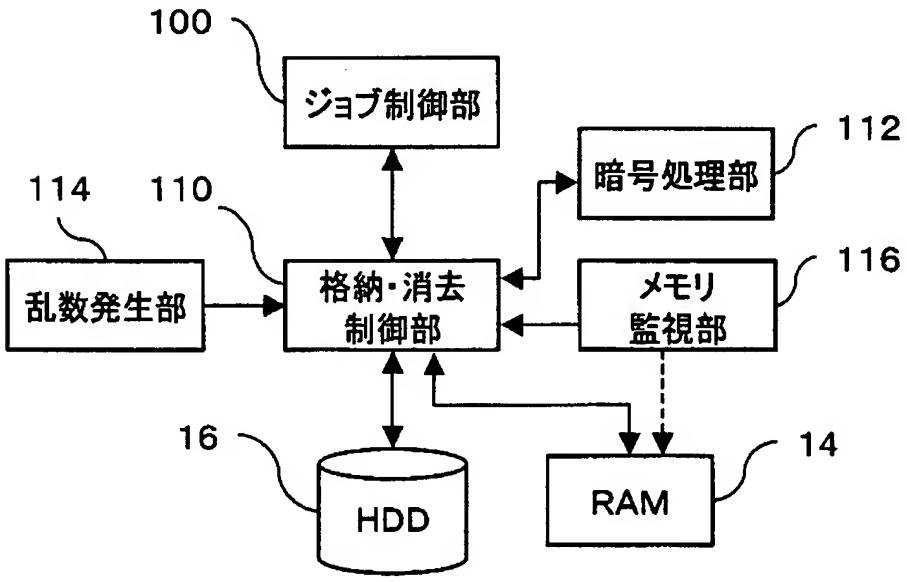
１０　ＣＰＵ、１２　ＲＯＭ、１４　ＲＡＭ、１６　ＨＤＤ（ハードディスク・ドライブ）、１８　操作パネル、２０　通信インタフェース、２２　スキャンエンジン、２４　プリントエンジン、４０　格納ファイル、４２　格納ファイルの一部分。

【書類名】　　図面

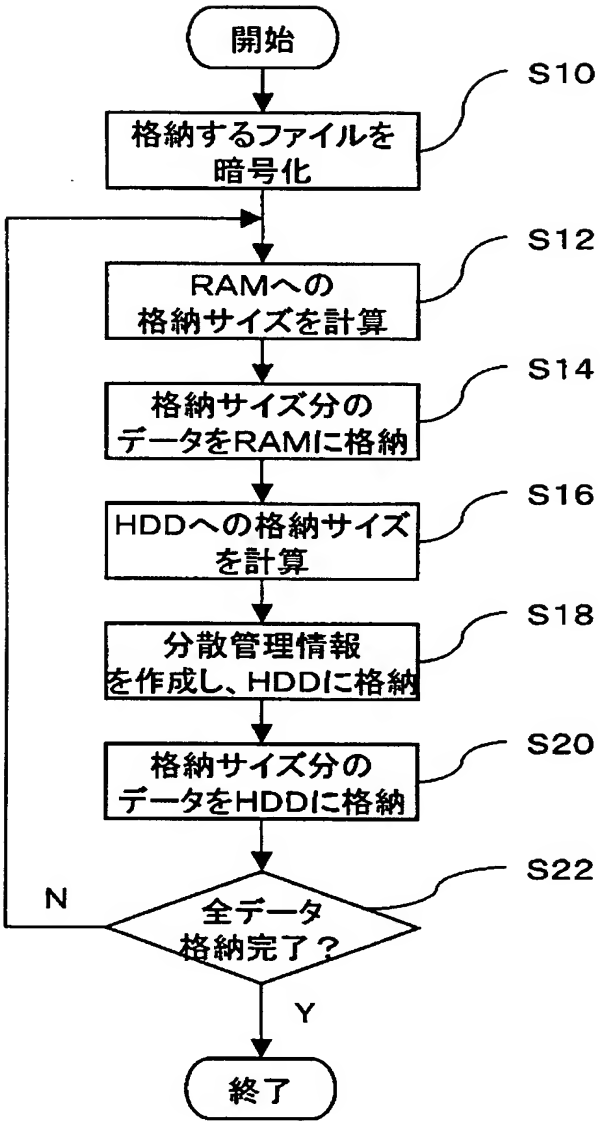
【図１】


10
18
操作
パネル
12
ROM
14
20
通信
インタフェース
RAM
42
格納ファイル
の一部分
CPU
22
スキャン
エンジン
16
HDD
24
40
プリント
エンジン
格納ファイル

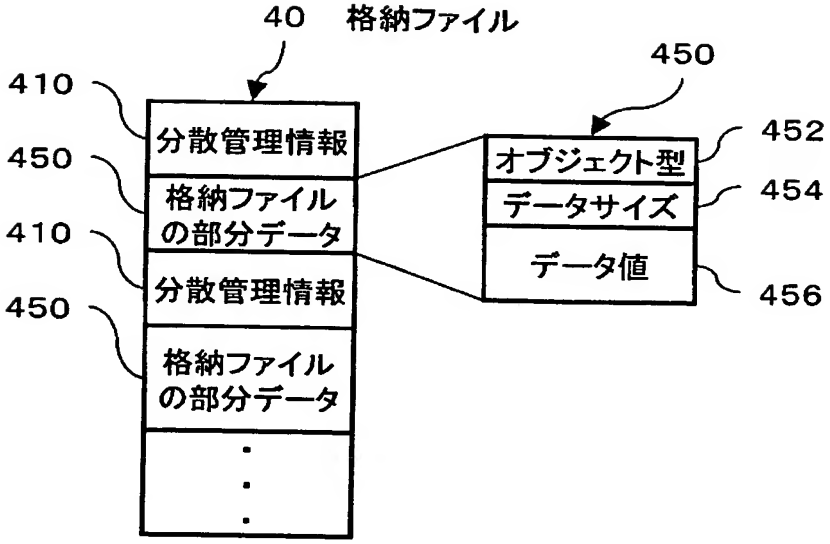
【図２】


100
ジョブ制御部
112
暗号処理部
114
110
乱数発生部
格納・消去
制御部
メモリ
監視部
116
16
HDD
RAM
14

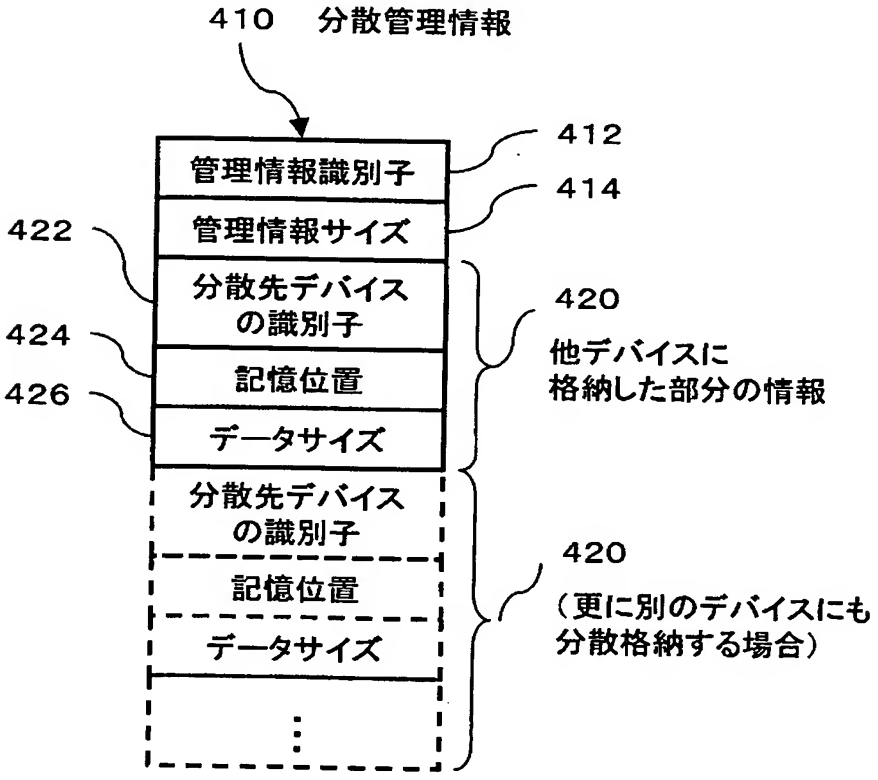
【図３】


開始
S10
格納するファイルを暗号化
S12
RAMへの格納サイズを計算
S14
格納サイズ分のデータをRAMに格納
S16
HDDへの格納サイズを計算
S18
分散管理情報を作成し、HDDに格納
S20
格納サイズ分のデータをHDDに格納
S22
全データ格納完了？
N
Y
終了

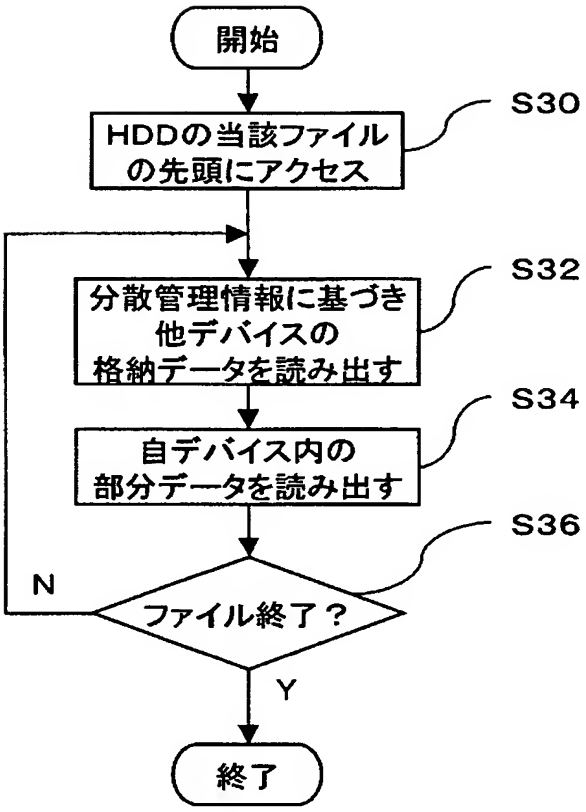
【図４】


40　格納ファイル
410
分散管理情報
450
格納ファイル
の部分データ
410
分散管理情報
450
格納ファイル
の部分データ
450
オブジェクト型
データサイズ
データ値
452
454
456

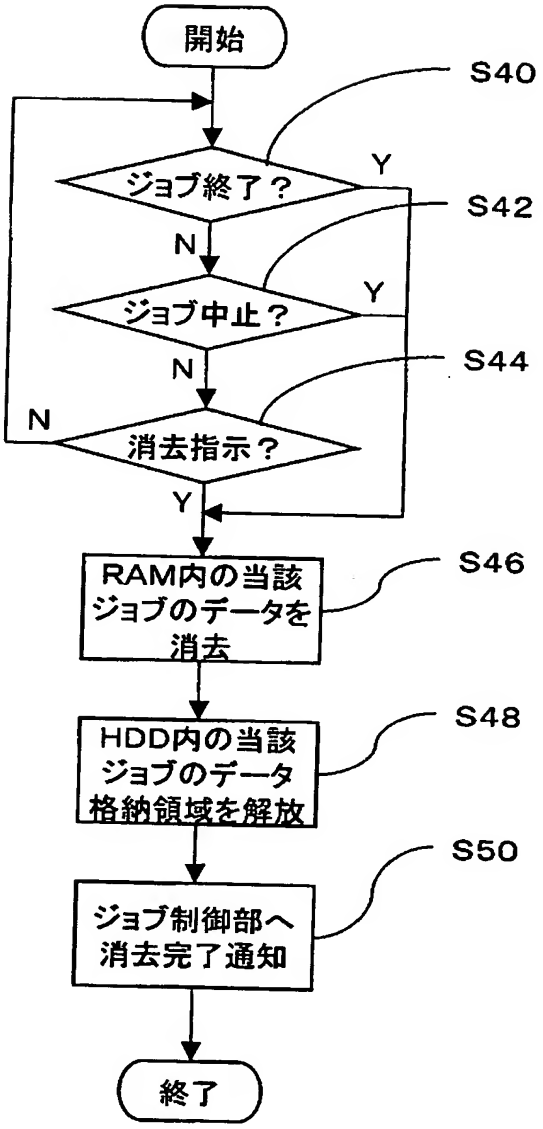
【図５】


410　分散管理情報
管理情報識別子
管理情報サイズ
分散先デバイス
の識別子
記憶位置
データサイズ
分散先デバイス
の識別子
記憶位置
データサイズ
412
414
422
424
426
420
他デバイスに
格納した部分の情報
420
（更に別のデバイスにも
分散格納する場合）

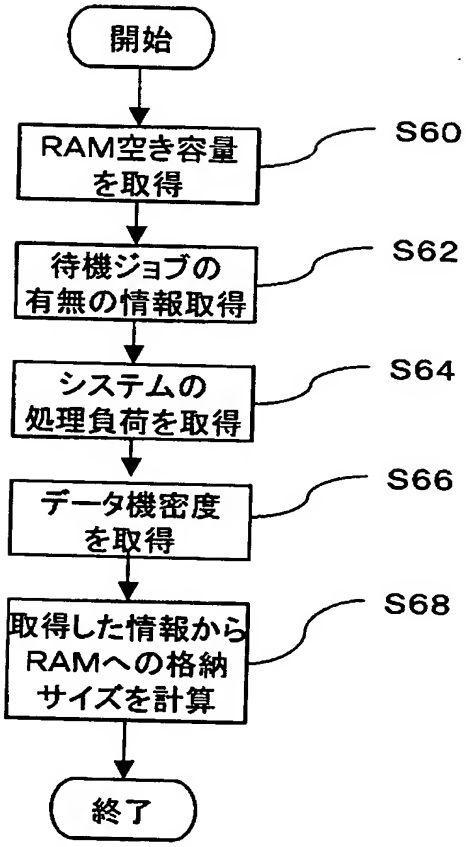
【図６】


開始
HDDの当該ファイルの先頭にアクセス
S30
分散管理情報に基づき他デバイスの格納データを読み出す
S32
自デバイス内の部分データを読み出す
S34
ファイル終了？
S36
N
Y
終了

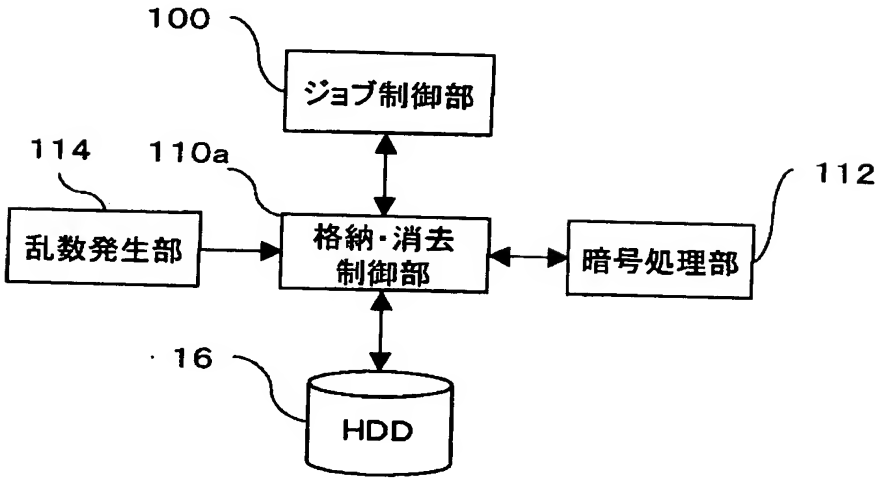
【図７】


開始
S40
ジョブ終了？
Y
N
S42
ジョブ中止？
Y
N
S44
消去指示？
N
Y
RAM内の当該ジョブのデータを消去
S46
HDD内の当該ジョブのデータ格納領域を解放
S48
ジョブ制御部へ消去完了通知
S50
終了

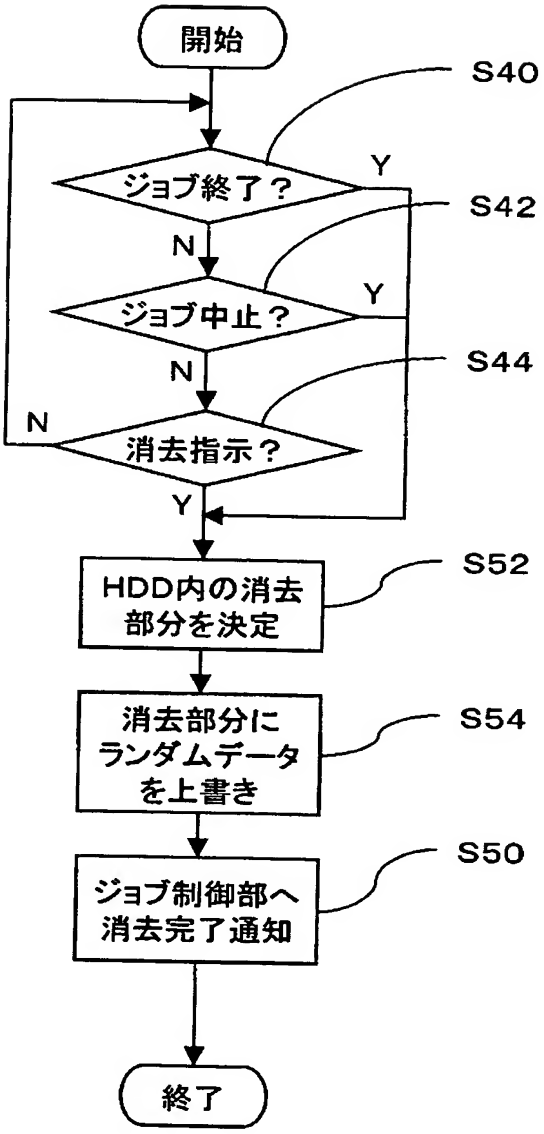
【図８】


開始
RAM空き容量を取得
S60
待機ジョブの有無の情報取得
S62
システムの処理負荷を取得
S64
データ機密度を取得
S66
取得した情報からRAMへの格納サイズを計算
S68
終了

【図９】


100
ジョブ制御部
114
110a
112
乱数発生部
格納・消去制御部
暗号処理部
16
HDD

【図１０】


開始
S40
ジョブ終了？
Y
S42
N
ジョブ中止？
Y
S44
N
消去指示？
N
Y
S52
HDD内の消去部分を決定
S54
消去部分にランダムデータを上書き
S50
ジョブ制御部へ消去完了通知
終了

【書類名】　要約書

【要約】

【課題】　画像形成装置等のジョブ処理装置内の大容量記憶装置に格納されるジョブデータのセキュリティを高める。

【解決手段】　ＣＰＵ１０は、ジョブの実行に必要なジョブデータを保存する際には、そのジョブデータに暗号化を施した上で、その一部分４２をＲＡＭ１４に格納し、残りの格納ファイル４０をＨＤＤ１６に格納する。ジョブが終了したときには、ＲＡＭ１４内の当該ジョブのジョブデータの一部分４２を消去する。この消去によりジョブデータ４２の一部分は完全に消滅するので、仮にＨＤＤ１６を抜き出して調査されても、完全なジョブデータを知られることはない。

【選択図】　図１

特願２００３－０８１４４５

出　願　人　履　歴　情　報

識別番号　　［０００００５４９６］

１．変更年月日　　１９９６年　５月２９日
［変更理由］　　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社